CLAIMS:

1. A method of determining proximity of a target node to a source node, comprising:

communicating a query from the source node to the target node,

communicating a first response from the target node to the source node, immediately after the query is received at the target node,

receiving the first response at the source node,

processing the query at the target node to produce therefrom a second response that facilitates a verification of the target node and its first response,

communicating the second response from the target node to the source node,

determining a measure of communication time between communicating the query and receiving the first response, and

determining the proximity of the target node based on the measure of communication time.

2. The method of claim 1, wherein

the query and at least one of the first and second responses correspond to at least a portion of a cryptographic key-exchange protocol.

3. The method of claim 2, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

4. The method of claim 1, wherein

the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol.

5. The method of claim 1, wherein

the query includes an encryption of an item based on a public key of the target node, and

the processing of the query includes decrypting the item based on a private key of the target node, for inclusion in the second response.

6. The method of claim 5, wherein

the first response includes a random number, and

the processing of the query further includes encrypting the item and the random number using a public key of the source node to form at least a portion of the second response.

7. The method of claim 5, wherein

the first response includes an encryption of a random number based on a public key of the source node.

8. The method of claim 1, wherein

determining the proximity includes comparing the communication time to a threshold value that distinguishes between local and remote nodes.

9. The method of claim 1, further including

restricting communications with the target node based on the proximity.

10. The method of claim 1, further including

restricting access of the target node to system resources based on the proximity.

11. A node on a network including:

a communication device that is configured to receive a query from a source node and to transmit a first response that facilitates proximity verification of the node, to the source node upon receipt of the query, and a second response that facilitates a verification of the node to the source node, and

a processor that is configured to process the query and produce therefrom the second response.

12. The node of claim 11, wherein

the processor is configured to process the query and produce the response as part of a cryptographic key-exchange protocol.

13. The node of claim 12, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

14. The node of claim 11, wherein

the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol initiated by the source node.

15. The node of claim 11, wherein

the query includes an encryption of an item based on a public key of the node, and

the processor is configured to decrypt the item based on a private key of the node, for inclusion in the second response.

16. The node of claim 15, wherein

the first response includes a random number, and

the processor is configured to encrypt the item and the random number using a public key of the source node to form at least a portion of the second response.

17. The node of claim 15, wherein

the first response includes an encryption of a random number based on a public key of the source node.

18. A node on a network including:

a communication device that is configured to transmit a query to a target node and to receive a first response and a second response from the target node,

a processor that is configured to:

measure a communication time between transmitting the query and receiving the first response,

determine a proximity of the target node relative to the node based on the communication time, and

verify the target node based on the second response.

19. The node of claim 18, wherein

the processor is configured to generate the query and process at least one of the first and second responses as part of a cryptographic key-exchange protocol.

20. The node of claim 19, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

21. The node of claim 18, wherein

the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol initiated by the node.

22. The node of claim 18, wherein

the query includes an encryption of an item based on a public key of the target node, and

the second response includes a decryption of the item based on a private key of the target node.

23. The node of claim 22, wherein

the first response includes a random number, and

the second response includes an encryption of the decryption of the item and the random number, using a public key of the node.

24. The node of claim 23, wherein

the second response further includes a signature of the decryption of the item and the random number, using a private key of the target node.

25. The node of claim 22, wherein

the first response includes an encryption of a random number based on a public key of the node.

26. The node of claim 18, wherein

the processor is configured to determine the proximity based on a comparison of the communication time to a threshold value that distinguishes between local and remote nodes.

27. The node of claim 18, wherein

the processor is further configured to control subsequent communications with the target node based on the proximity.

28. The node of claim 18, wherein

the processor is further configured to control access of the target node to system resources based on the proximity.